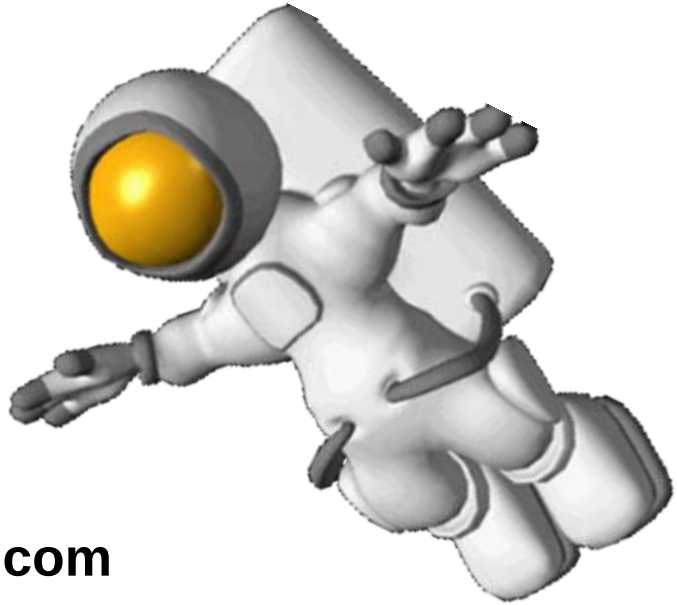
Information Technology Infrastructure Committee (ITIC)
Report to NAC



Al Edmonds

aedmonds@logapp.com

OUTLINE

- Committee Members
- Meeting – 4/15/2010 and 4/16/2010
- Future meetings (ITIC & ASCS)
- Cyber security
- High Performance Computing
- Revised Work Plan
- Questions/Comments
- Observations

Committee Members

- **Membership**
  - Ret. General Albert (Al) Edmonds (Chair), President - Edmonds Enterprise Services, Inc.
  - Mr. Alan Paller, Research Director - SANS Institute
  - Dr. Robert Grossman, Professor – University of Illinois
  - Dr. David Waltz, Director, CCLS – Columbia University
  - Dr. Larry Smarr, Director – California Institute for Telecommunications and Information Technology
  - Dr. Charles Holmes, Retired – NASA
  - Ms. Debra Chrapaty, Senior VP – CISCO
  - Dr. Alexander Szalay, Professor – Johns Hopkins University
  - Dr. Alexander H. Levis, Professor - George Mason University

  - Ms. Tereda J. Frazier (Exec Sec), Special Assist. to CIO, NASA

April 15th and 16th MEETING

- **Meeting**
  - Location: NASA Headquarters, Rm. 2O43
  - Meet-Me-Number available for virtual members

- **Presentations from the following areas:**
  - IT Security Operations
  - ASCS Status Briefing
  - Status of NASA Supercomputing
  - IT Summit Briefing
  - IT Governance
  - Making IT Stellar at NASA
  - Revised ITIC Work Plan
  - Logistics for future meetings

Future Meetings

- **ITIC Meetings**
  - Ad-hoc groups visiting centers to meet with NASA operational function personnel to have fact finding discussions
  - Next planned ITIC FACA meeting is July 27th as a telecon
  - Last planned ITIC FACA meeting for FY10 is September 28th and 29th, location TBD

- **ASCS Meetings**
  - Next meeting scheduled for May 14th and 15th, at NASA Headquarters
  - Remaining meeting schedules for FY10 are TBD

Cyber Security - The Threat Actors

- **NASA is an interesting target:**
  - Between 2007 and 2009, NASA on average logged nearly 1 billion vulnerability scans of its network perimeters on a monthly bases
- **NASA is witnessing attacks perpetrated by threat actors from all categories**
  - Criminal Groups
  - Ankle Biters, Script Kiddies, and Hacktivist
  - Nation States
- **Together, these actors instigated:**
  - 1,120 incidents between FY 2007 and 2008
  - 2,844 incidents between FY 2008 and 2009

Cyber Security - Threat Actions and Vectors

- **Threat actors exploited vulnerabilities using a number of well known threat actions and vectors:**
  - Web applications that have common security vulnerabilities
  - Spear Phishing, with email as a vector. Spear phishing attacks are designed to acquire credentials or create a back door on the compromised system and surreptitiously exfiltrate data
  - Phishing, with email as the primary vector and social engineering as a secondary vector. Phishing attacks are designed to steal personally identifiable information or user credentials
  - Exploitation of improper configurations with network devices as the vector

Cyber Security - Enterprise Risk Management

- **As NASA's foremost IT risk management entity, the IT Security Division is developing an all sources IT security risk assessment. The assessment focuses on three risk impact areas:**
  - Data loss
  - Disruption to enterprise services
  - Disruption to mission operations
- **Classic risk formula, Threat x Vulnerability x Likelihood x Impact = Risk**
- **All sources include:**
  - Security Operations Center (SOC) incident information, Cyber Threat Analysis Program (CTAP) reports, Cyber Counter Intelligence/Counter Terrorism (CI/CT) reports and classified channels

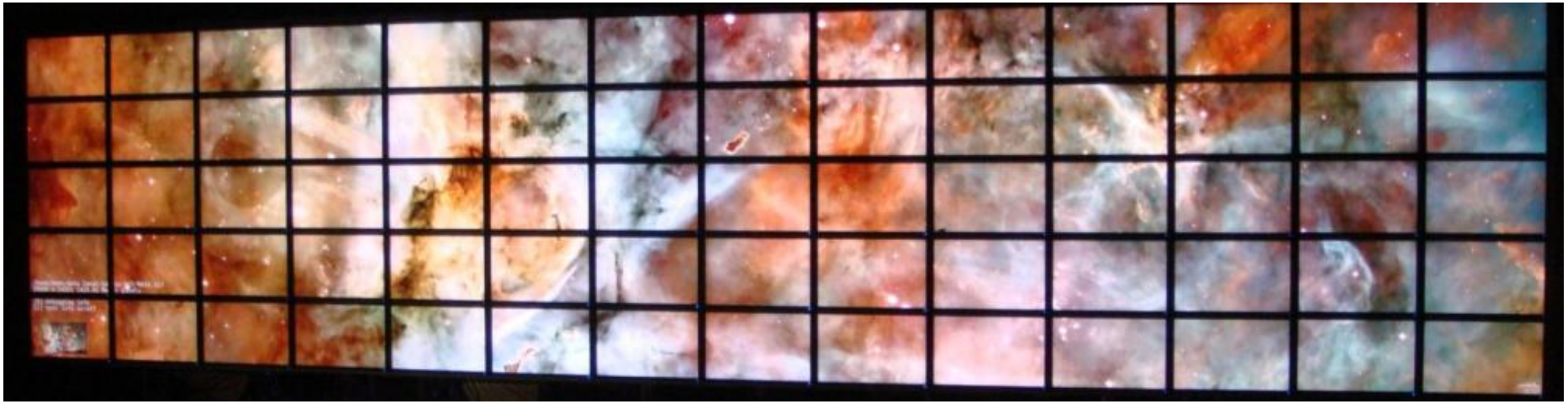
High Performance Computing

Linking the Calit2 Auditoriums at UCSD and UCI with LifeSize HD for Shared Seminars

High Performance Computing

Very Large Images Can be Viewed Using CGLX's TiffViewer

Spitzer Space Telescope (Infrared)

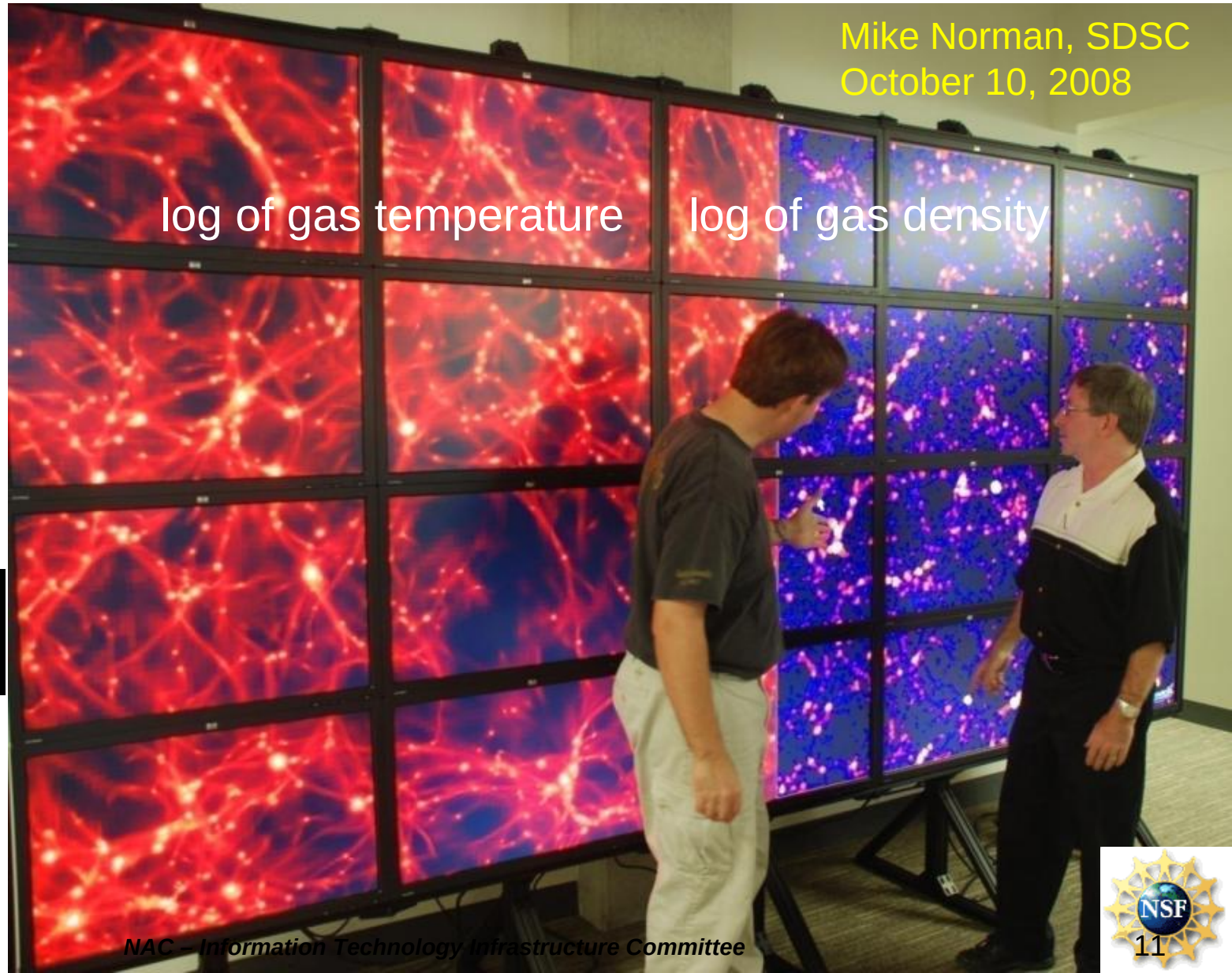


Hubble Space Telescope (Optical)
Source: Falko Kuester, Calit2@UCSD

High Performance Computing

Providing End-to-End CI for Petascale End Users

Two 64K Images From a Cosmological Simulation of Galaxy Cluster Formation



High Definition Video Connected OptIPortals: Virtual Working Spaces for Data Intensive Research

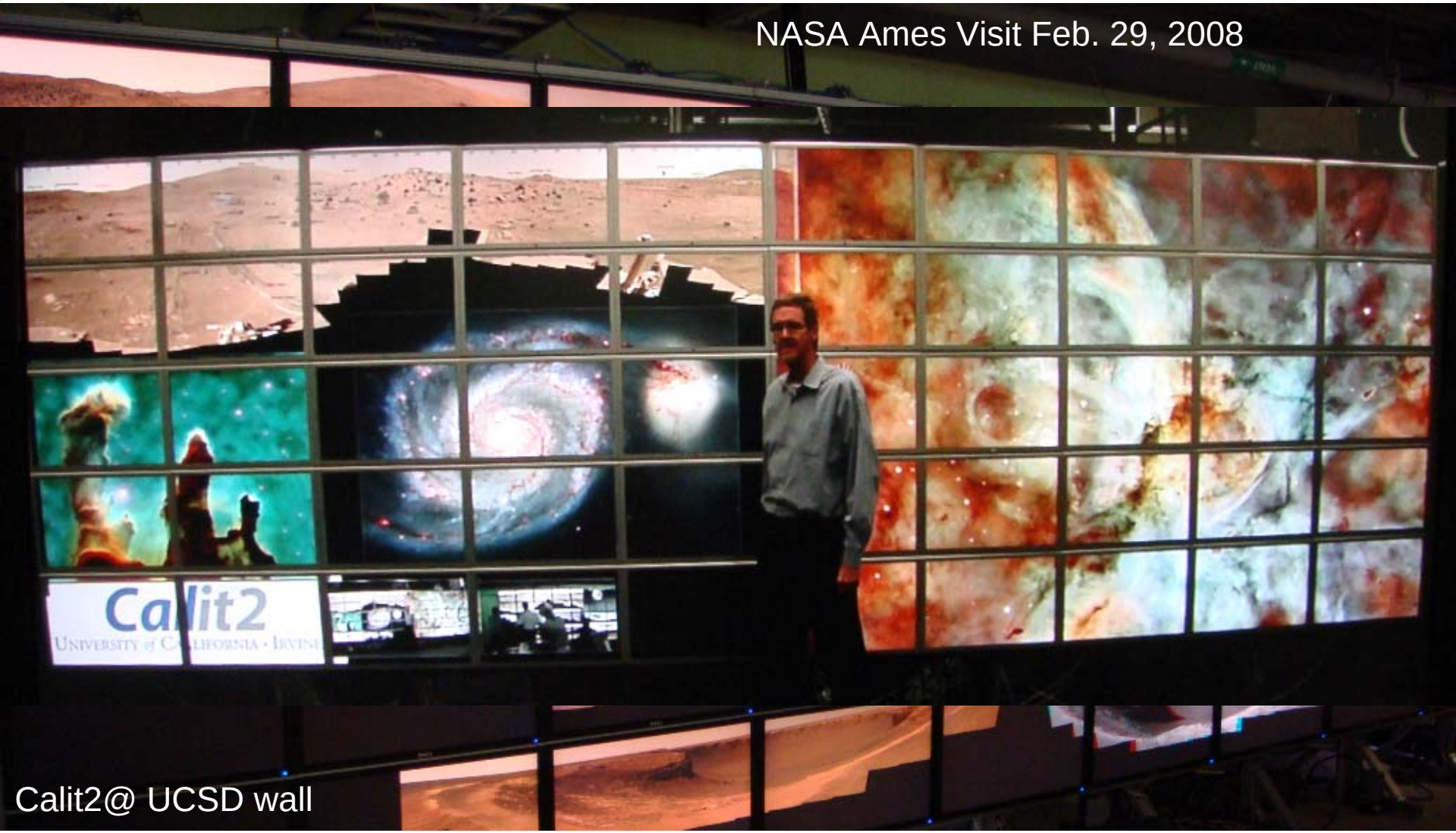
NASA Interest in Supporting Virtual Institutes

CGLX

LifeSize HD

NASA Ames
Lunar Science Institute
Mountain View, CA
Source: Falko Kuester, Kai Doerr Calit2; Michael Sims, NASA

Toward a Data and Visualization Intensive Working Environment Across Remote Sites

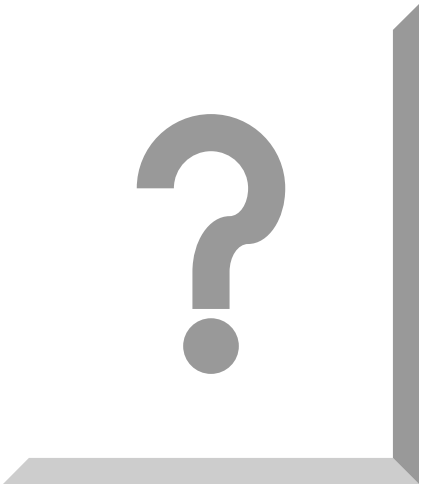


UCSD cluster: 15 x Quad core Dell XPS with Dual nVIDIA 5600s
UCI cluster: 25 x Dual Core Apple G5

Revised Work Plan

- Examine the ongoing and planned efforts for the IT Infrastructure and mission areas.
- Develop recommendations for an investment strategy for updating the infrastructure while greening it and at the same time reduce lifecycle costs.
- Investigate the state of NASA's high performance networks, high performance computing systems, and data intensive computing systems.
- Investigate the state of NASA's software and infrastructure support for collaborative teams.
- Examine NASA's data and communications environment for its aerospace operations and point out areas in need of attention.
- Examine the role of the OCIO, its strategic plans and projected resources, and IT governance across NASA.
- Creating green cloud computing.

Questions or Comments



Early Observations on NASA Security vis-á-vis Other Agencies

NASA Differences from Other Agencies

- **Negative: very high number of separate systems subject to security requirements**
- **Positive: access to situational awareness data on nearly every system (not mission systems yet)**
- **Positive: leadership – technical skills that identify actual attack vectors, sense of urgency**

Possible Findings

- **More than $12 million is being spent on out-of-date security compliance reports and can be shifted into continuous monitoring and improvement.**
- **Security is not being engineered effectively into systems at the beginning of and throughout the design/development process, increasing the costs and reducing the impact of bolting it on later.**
- **Security audits that find dozens of specific problems on individual machines do not lead to broad cost-effective changes.**

Short term task plan

- Briefings on security at the centers
- Briefings on how security can be introduced at the beginning of planning and development for major systems
- Meeting in May at headquarters on the day before cyber security subcommittee meeting